Installation Manual for the DiskGO™ 3.5” Network Hard Drive

This product is backed by a one year limited warranty.
For complete warranty information visit
www.edgetechcorp.com/register

IMPORTANT
PLEASE CONTACT A QUALIFIED TECHNICIAN FOR ASSISTANCE IN INSTALLING OR USING THIS PRODUCT IF YOU ARE NOT FAMILIAR WITH DOING SO. ANY INSTRUCTIONS INCLUDED WITH THE PRODUCT ARE FOR CONVENIENCE ONLY AND ARE NOT INTENDED TO BE ALL-INCLUSIVE.

EDGE™
TECH | CORP

327 East 14th Street / Ada OK 74820 / (800) 332-6581 / (580) 332-6581 / www.edgetechcorp.com

TABLE OF CONTENTS

Getting Started

Configuring your DiskGO 3.5” Network Hard Drive

ADMINISTRATION

SHARE MANAGEMENT

DISK MANAGEMENT

NETWORKING

- LAN
- DHCP Server
- Static IP

PRINTERS

- Setting the DiskGO 3.5” Network Hard Drive as a Print Server
- Adding the Printer in Windows
- Printer Troubleshooting

Getting Started

Overview

The DiskGO 3.5" Network Hard Drive is a broadband network attached storage (NAS) device designed for use on a small office/home office (SOHO) network. With the DiskGO 3.5" Network Hard Drive connected to the network, users can easily and quickly access, store, and share digital files. Also, home users can access or transfer files on digital devices such as set-top TV boxes, digital cameras, camcorders, digital audio players, and more by directly connecting such devices to the USB port on the DiskGO 3.5" Network Hard Drive.

Package Contents

- DiskGO 3.5" Network Hard Drive
- DC Power Adapter, 12v
- Stand
- Cat5 Cable
- Install CD
- Quick Install Guide
- User Guide (on CD)

System Requirements

- Windows XP, 2000, ME, 98, Mac OS X+
- Web Browser (such as Internet Explorer or FireFox)
- Network router with DHCP server
- Open RJ-45 Network Connection

Installation of the DiskGO 3.5" Network Hard Drive

With the enclosed Ethernet cable, connect the DiskGO to an open port in the router on the network. Make sure the DHCP server function on the router is enabled, and the networked PC is configured as a DHCP client.

1. Plug in the DC power adapter to the DiskGO. Wait for 30 ~ 60 seconds until the blue LED light illuminates.
2. To access the DiskGO, double click "My Computer" on any computer attached to the network, and type "\\DiskGO" in the address bar. Double click the folder "DiskGO." This will allow any network PC to access files on or save files to the DiskGO.

Initial Setup (without Install CD)

The DiskGO 3.5" Network Hard Drive gives advanced users the capability to easily configure privacy and security access levels in folders, monitor power usage, set up a Redundant Array of Independent Disks or RAID with an external USB Hard Drive & monitor status of the HDD. Use of the Configuration & Administration pages is optional. To simply share files over the network, these configuration pages are not needed. *The Configuration & Administration pages are recommended for advanced users only.*

To open the configuration page, type “http://Diskgo” in the address bar of a browser (e.g., Internet Explorer or Firefox). Then click the button to enter the administration configuration page.

CONFIGURING YOUR DiskGO 3.5” Network Hard Drive

The Administrator user interface has six main menus for configuring the DiskGO 3.5” Network Hard Drive:

- **Administration**
    - Basic
    - Firmware Administration
    - Alerts Logging
    - Windows Setup
    - User Management

- **Share Management**
    - Basic
    - Create Share
    - Share Access

- **Disk Management**
    - Basic
    - Legacy Disks
    - Create New Pool
    - Resize Pool
    - Add Mirrors
    - Remove Mirrors
    - Power Management

- **Networking**
    - LAN

- **Printers**

Notes:

• To view the pages associated with each main page, move your cursor over page names across the top of the user interface. To go to a particular page, click the page name.

• If you are satisfied with the configuration settings you have made on each configuration page, click **Apply** before going to another configuration page. If not, click **Cancel.**

ADMINISTRATION

BASIC

On the Administration - Basic page, you can view and modify the following basic DiskGO administration settings:

- DiskGO machine
- Administration user name **(preset to edgetech)**
- Administration password **(preset to admin)**
- DiskGO Time
- Browser Time
- Time Zone Region
- Time Zone Country
- Time Zone City
- NTP servers

The DiskGO software keeps track of the date and time and uses this information to timestamp files and for administrative purposes such as error and connection logging. The DiskGO clock runs in real time and has a battery to keep the clock running even when the power to the DiskGO is turned off.

The current date and time as recorded by both the DiskGO and the PC connected to the device is displayed. To manually set the DiskGO time, click **Set Time Manually**. To set the DiskGO time to match the PC connected to the DiskGO Share, click **Set DiskGO Time to Match**.

The DiskGO 3.5" Network Hard Drive is also capable of synchronizing the date and time settings on the network. DiskGO drives which are on networks connected to the Internet should usually be set up to do this. This kind of network time synchronization is done through an international standard called Network Time Protocol (NTP). There is space opposite **NTP Servers** to type the IP addresses of three machines for the DiskGO to use in determining the current date and time. The default IP addresses are 192.5.41.40, 192.5.41.41, and 133.100.9.2. The first two of these IP addresses is a server run by the United States Naval Observatory as a public service to provide the precise time over the Internet, and the third is a similar time server in Japan.

Use the spaces opposite the **Time Zone Region**, **Time Zone Country**, and **Time Zone City** to make local time zone settings.

To perform a software reboot of the DiskGO, click **Reboot**.
To restore the DiskGO to the factory settings, click **Restore Defaults** *(this option does not delete any digital files saved on the DiskGO).*

FIRMWARE

On the Firmware Administration page, you can view the current DiskGO firmware version and upgrade the firmware to a newer version, if available. Always note the version information when contacting technical support.

To update the firmware

1. Download the new version of the firmware to a PC that is connected to the DiskGO.
2. Click **Browse**.
3. Click the name of the downloaded file, and then click **Open**.
4. Click **Upgrade***.

***Caution!** The upgrade process takes several minutes. Do not turn off the DiskGO while the upgrade is in progress! Doing so could corrupt the DiskGO software, making it impossible for the DiskGO to boot or to upgrade the firmware in the future. If you do accidentally turn off the DiskGO while the upgrade is in progress, contact EDGE technical support for help (www.edgetechcorp.com/support).*

ALERTS LOGGING

This section allows the user to receive emails if an error occurs within the DiskGO 3.5" Network Hard Drive. First check the **E-mail Notification Enabled** box at the top of the page. Next enter the SMTP server address in the **Error Handling SMTP Server** box. The SMTP server is a server that accepts incoming e-mail for routing to its intended recipient. This is usually NOT the same as any part of the email address; it is a server that is used for all addresses. Usually, your ISP will provide the server name. The name of the SMTP server is also required by your e-mail client program such as Outlook or Eudora.. If you are uncertain what your SMTP server address is, try looking at your email client settings and use the same address. Once the address is set the DiskGO will email the listed email addresses if an error should occur within the device . To test, click on the **Send Test E-Mail** button.

To set Pop-Up notifications, check the **Pop-Up Notification Enabled** box. Next, enter the Windows Network ID names of the computers that you wish to receive the message. Please note that pop-up messages must be enabled on each machine in order for them to receive the message. Windows messaging is turned off by default on Windows XP.

WINDOWS SETUP

On the Windows Setup page, you can set up how the DiskGO 3.5" Network Hard Drive participates in a Windows environment:

- **Workgroup Member mode** (default)
- **Domain Member mode**
- **Primary Domain Controller** (PDC) mode

Note: The available settings on the Windows Setup page depend on the type of mode that is selected.

Workgroup Member Mode

In Workgroup mode there are two options for limiting share access to important data:

- Password-based share access (PBSA)
- User-based share access (UBSA).

PBSA is a simple model that allows only users having the correct password to gain access to an individual share.

UBSA access is more flexible. An administrator can grant permissions to shares to each individual user. An individual user can be assigned either no access, full access, or read access on a share-by-share basis. If you select USBA, you must also designate a pool. The DiskGO uses this pool to save user information. If no disk pool exists, you must create one (see "Creating a New Disk Pool") before you select UBSA. **Note**: A pool is a specified amount of disk space that contains one or more shares (see "Disk Management" for information about creating and managing disk pools).

To configure a DiskGO as a member of a Workgroup

1. Select the **Workgroup Member Mode** checkbox.
2. Type the workgroup name in the **Workgroup Name** box.
3. Select either the **Password Based Share Access** check box or the **User Based Share**

Access check box. If you select the **User Based Share Access** check box, in the **Pool Name** list, click the pool where user accounts are stored.

Domain Member Mode

A domain is a workgroup with the added feature of single sign-on. With single sign-on, a user has one account that is shared across multiple computers. Also, the user can access resources on another computer without having to re-authenticate. Computers in a domain are controlled from a central location (domain controller) and users must obtain central authentication before joining the domain. If your network uses a domain, you may prefer to configure the DiskGO to connect to the network as a domain member. When the DiskGO is configured in this way, the DiskGO software sends a request to the PDC to authenticate users, which provides user-level security. Although the DiskGO can be in only one domain at a time, you can configure the DiskGO to connect to two different domains. This allows you to easily switch between the two domains using the same user name and password.

To configure the DiskGO 3.5" Network Hard Drive as a member of a domain

1. Select the **Domain Member Mode** check box.
2. Type the domain name in the **Domain Name** box.

If the DiskGO is recognized in this domain, the device rejoins the domain without authentication. Otherwise, you must type the domain administrator user name in the **Admin User** box and the password in the **Admin Password** box.

For DiskGO drives that are also configured to support Network File System (NFS), the DiskGO assigns UNIX® user IDs (UID) and group IDs (GID) to files created through the Common Internet File System (CIFS). User IDs are in the range 35000–40000; group IDs are in the range 42000–43000.

Primary Domain Controller Mode

A domain controller must exist on a network before you can create a domain. The domain controller is the repository of user information. Different versions of Windows have different levels of support for domain membership. Windows NT, Windows 2000 and Windows XP Professional fully support domain membership. Users of these versions of Windows can use a DiskGO to maintain user accounts and to use the additional security features of domains. Windows 98 and Windows ME provide limited domain membership support. Users of computers running on one of these Windows operating systems can have their account information served by a DiskGO, but they cannot use the additional security features of domains. Users of Windows XP Home Edition cannot use PDC support in any way.

To configure the DiskGO 3.5" Network Hard Drive as a primary domain controller

1. Select the **Primary Domain Controller Mode** check box.
2. Type the domain name in the **Domain Name** box. Users who want to join the domain must include the domain name in the logon information.
3. Type the administrator user name in the **Admin User Name** box. The administrator account is used to add, delete, and modify user and machine accounts in the domain. ***(The** administrator account is separate from the one used to access the DiskGO Share user interface.)*
4. Type the administrator password in the **Admin Password** box and again in the **Confirm Password** box.
5. Click a pool in the **Profiles and Scripts Pool** list.
6. Click a drive letter in the **Logon Drive** box.

- Each domain may have only one PDC. If a PDC already exists in a given domain, do not configure the DiskGO as a PDC+.

- When operating as a PDC, a DiskGO stores some data about each user on the disk. The DiskGO software creates two shares within the pool given here: profiles and netlogon.
- Only Administrators need to be aware of these shares to ensure that there is enough disk space.
- The netlogon share contains the logon script described in Step 6.
- For some versions of Windows, the operating system stores the user environment (window layout and menu items) in the profiles share.
- When a user logs on to the domain, the user home directory is assigned this drive letter. This is essentially an implicit **net use** command.

7. Type the name of the logon script in the **Logon Script** box.

Using the DiskGO 3.5" Network Hard Drive as a Primary Domain Controller

After the DiskGO is configured as a primary domain controller (PDC), you must add each computer to the domain. Open the Windows Help and Support Center for instructions on adding a computer to a domain.

Creating a User Account

1. Log off Windows and then log back on.
2. Type the PDC administrator user name and password in the appropriate boxes.
3. Click the new domain name in the **Log on to** box and click **OK**.
4. Open a command prompt window.
5. Type net user /add /domain <user name> <password>
   - <user name> is the user name you want to use, and <password> is the password you want to use.
6. Press ENTER.

Creating a Home Directory

Each user can create a home directory, which is a disk share that is dedicated to that particular user. Having a home directory enables the logon drive feature and the **/home** option on the Microsoft **net user** command. The logon drive is mapped only for those users that have created a home directory.

To create a Home Directory

Create a share and assign the user name as the share name. The share must reside on the PDC, but it can be in any of the PDC pools.

Creating a Group User Account

In Microsoft Windows, file access permissions may be given to individual users or to groups of users. A group can have any number of users, and users can be in any number of groups. When there are many users, the use of groups can simplify the administration of file permissions. For example, whatever file permissions are granted to the group also apply to the members of the group. As group membership changes, the administrator updates the group account to accommodate new members and denies access to those who have left the group.

Domain members rely on the domain controller to provide group membership information. When the DiskGO 3.5" Network Hard Drive is acting as a PDC, it maintains the group membership information. Group membership may be managed using the Microsoft **net group** command. To use the **net group** command, log on to Windows as the domain administrator and open a command prompt window. Examples 1 and 2 create new groups called nurses and doctors. Examples 3, 4, and 5 add individual nurses to these groups. Examples 6 and 7 delete individual users from the groups.

Examples:

1. net group /domain /nurses /add
2. net group /domain /doctors /add
3. net group /domain /nurses dean /add
4. net group /domain /nurses judy /add
5. net group /domain /doctors dawn /add
6. net group /domain /nurses dean /delete

7. net group /domain /doctors dawn /delete

The DiskGO automatically assigns all users to a group named **users**. It is not necessary to add users to the users group, and users cannot be deleted from the users group. The **net group** command cannot be used to query the members of the users group, but the **net users** query returns the same information. For DiskGO devices that are also configured to support NFS, DiskGO assigns UNIX user IDs (UIDs) and group IDs (GIDs) to files created through CIFS. User IDs are in the range 35000–40000; group IDs are in the range 42000–43000. Moreover, setting up permissions on a Windows platform and copying the file to a DiskGO disables your permissions.

Managing the Domain
Use the Microsoft **net user** command to add, delete, and modify user accounts. Use the Microsoft **net group** command to add, delete, and modify group accounts or to add and delete users memberships to groups.

Creating a Logon Script
The DiskGO 3.5" Network Hard Drive passes the name of the current user to the logon script when the script is run. This allows the script to run differently for different users. Use the "%1" replaceable parameter to access the user name. After you have access to the netlogon share, you must create the logon script. It must reside within the netlogon share that the DiskGO automatically creates in the pool given in "Profiles and Scripts Pool." You can include directory names within the script name, but the path must be relative (the path cannot start with a drive letter or a slash). For example, if you type netlogon.bat, when you have access to the netlogon share, you must create a file named netlogon.bat. Or if you type scripts/netlogon.bat, you must create both a directory named scripts as well as the netlogon.bat file.

Note: All files on the DiskGO have permissions for the user who owns the file, a default primary group, and Everyone. Separate permissions can be added for individual users using Windows access control list (ACLs). The default primary group is always users and cannot be changed. For the current release, there is no reason to create a group account.

USER MANAGEMENT

The User Management page allows an administrator to manage user accounts when UBSA mode is enabled, and the DiskGO is set up to operate in Workgroup Member mode.

To add a new user

1. Click **Create New User**.
2. Type the name of the user in the **New User Name** box.
3. Type the login password for the new user in the **Login Password** box and again in the **Confirm Password** box.
4. In the **Shares Permissions** box, click the permissions to be granted to the new user.

5. Click **Create User**.

SHARE MANAGEMENT

A share is a directory that can be mounted on one or more computers and filled with as many subdirectories as desired, limited only by the space in the disk pool in which the share exists.

A pool is a specified amount of disk space that contains one or more shares (see "Disk Management" for information about creating and managing disk pools).

If more than one share is in the same pool, any space taken up by one share is space that is not available for the other shares in that pool, and if any one share fills up the space, no files can be written to any of the shares in that pool until some files are deleted. Shares in other pools however, continue functioning normally as long as there is available space in the other pools.

The DiskGO 3.5" Network Hard Drive supports the Microsoft file allocation table (FAT) file system. If a disk is claimed using the FAT system, the entire disk is a considered as a single share. A disk using the FAT system is called a legacy disk (see "Legacy Disk Management – Basic) and a legacy disk share is called a foreign share.

Otherwise, a share is called a pool share. Administrators can control how each share is accessed. DiskGOs support four protocols for accessing shares:

- Common Internet File System (CIFS)
- Network File System (NFS)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)

Windows machines use CIFS protocol, UNIX-based machines typically use NFS, and Web browsers use HTTP. FTP is an older internet protocol supported by both browsers and command-line-based clients. Each of these protocols can be disabled globally. If they are enabled globally, they may be enabled or disabled independently for each share. Moreover, in workgroup modes (see "Workgroup Member Mode"), administrators can control which individuals can access each share. In PBSA mode, only individuals who know the share password can access the share. In UBSA mode, read, read/write, or no access permissions may be granted to each individual user.

Note: A disk pool must be created before a share can be created (see "Disk Management").

BASIC

The Share Management: Basic page lists all the shares on the DiskGO 3.5" Network Hard Drive and the access permissions for each share.
Global Access Info:. Lists the permissions for each file access protocol.

Shares: Lists the pools shares, which are grouped by pool.
Legacy Disk Shares: Lists foreign shares (if any exist).
The CIFS and NFS protocols are read-only, unless write permission is granted. Similarly, the FTP and HTTP protocols are read-only, unless create and/or delete permission is granted. The create permission allows users to create new files but not alter existing files.

The delete permission allows users to modify and delete existing files. If a share has delete permission but not create permission, users can modify or delete files, but cannot add them.
To rename an existing share, click **Rename Share**.
To create a new share, click **Create New Share**.

CREATE SHARE

The Create New Share page allows you to create a new share in an existing pool.
In Workgroup Member mode with PBSA, the Enable Share Authentication security feature should be enabled. When enabled, this feature provides share-level security through password protection of Windows shares. In Workgroup Member mode with UBSA, users are listed under share permissions. This feature provides control access to the newly-created share on a user-by-user basis. If more-advanced security features are required, configure the DiskGO as a domain controller (See "Primary Domain Controller).

To create a new share in Workgroup Member mode with PBSA

1. Type the name of the new share in the **New Share Name** box.
2. In the **Create in Pool** list, click the pool where the new share is to be located.
3. Select the **Enable Share Authentication** check box to password protect the share. Otherwise, the share can be accessed by anyone that is able to connect to the device.
4. Type the password in the **Share Password** box and again in the **Confirm Password** box.
5. Click **Create Share**.

To create a new share in Workgroup Member mode with UBSA

1. Type the name of the new share in the **New Share Name** box.
2. In the **Create in Pool** list, click the pool where the new share is to be located.
3. Opposite **Shares Permissions**, click the permission type to be granted to each user.
4. Click **Create Share**.

SHARE ACCESS

The Share Access page allows an administrator to view and modify share access. This page is available only if the DiskGO has been configured as a member of a workgroup. It is not available if the DiskGO has been configured as a member of a domain or as a domain controller. If PBSA has been set for the workgroup, the content of the Share Access page is different than if UBSA has been set for the workgroup.

To change the share access settings of an existing share for a workgroup with PBSA

1. In the **Share Name** list, click the name of the share.
2. Click the **Enable Share Authentication** check box to change the setting. Selecting the check box enables password-protected access; clearing the check box disables password-protected access, allowing open access.
3. Click **Apply**.

To change the password of a password-protected share

1. Type the new password in the **New Password** box and again in the **Confirm Password** box.
2. Click **Apply**.

To change share access settings of an existing share for a workgroup with UBSA

1. In the **Share Name** list, click the name of the share.
2. In the **Share Permissions** list, click the permission type to be granted to each user.

DISK MANAGEMENT

BASIC

On the Disk Management - Basic page, you can do the following:

- View a graph showing the disks that are connected to the DiskGO (both the DiskGO and other connected USBs) and how the space on those disks is allocated

View disk pool mapping information, which includes:

- The name, type, and status of the pools
- The logical size, space used, and physical size of the pools
- The amount of space on each disk that is allocated to each pool

Create a new disk pool (see "Creating a New Disk Pool")
Rename a disk pool (see "Renaming a Disk Pool")
View detailed information about each disk
Rename a disk (see "Renaming a Disk")
Erase a disk (see "Erasing a Disk")
DiskGOs can be configured to automatically use new blank disks in certain ways (see "Configuring Default Disk Behavior").

The DiskGO 3.5" Network Hard Drives uses the Self-Monitoring Analysis and Reporting (SMART) protocol to query detailed information from each disk that supports SMART (most modern hard disks support SMART). SMART enables the DiskGO to alert users if disk failure is imminent, which gives users an opportunity to back up the data on the disk and to replace the disk. To view the disks that are available, select the **Show Disk Details** check box.

Renaming a Disk

1. On the Disk Management - Basic page, select the **Show Disk Details** check box, and then click **Rename Disk**.
2. In the **Old Disk Name** list, click the name of the disk that you want to rename.
3. Type the new name in the **New Disk Name** box.
4. Click **Rename Disk**.

Erasing a Disk

The Erase Disk function erases the data on a disk. When you wipe a disk, ensure that all the pools in the target disk that span multiple disks have either been deleted or that these companion disks are also being wiped at the same time. If this condition is not met, an error is the result.

To erase disks

1. Select the **Show Disk Details** check box, and then click **Erase Disk**.
2. Select the respective check boxes for the disks to be included in the wipe operation.
3. Click **Quick Erase** to remove only the control information from the disk. Click **Full Erase** to completely erase all the data from the disk.

Notes:

• The Full Erase process is very slow; the amount of time required for a full erase depends on the size of the disk.

• For the full erase operation to proceed, you must type **Yes, destroy everything on this disk** in the **Confirmation String** box.

Renaming a Disk Pool

1. On the Disk Management - Basic page, click **Rename Pool**.
2. In the **Old Pool Name** list, click the name of the pool that you want to rename.
3. Type the name of the new pool in the **New Pool Name** box.
4. Click **Rename Pool**.

LEGACY DISKS

The Legacy Disks page displays information about any attached legacy disks. Before you remove a legacy disk, click **Safely Remove Disk**. To return to the Legacy Disk Management page, click **Continue**.

CREATE NEW POOL

To create a new pool within the DiskGO 3.5” Network Hard Drive, open the **Create New Pool** page located within the **Disk Management** menu and follow the steps below. This procedure creates a basic, unencrypted pool. To create a **Mirrored, Striped or Encrypted pool,** follow the steps outlined in the following sections.

1. **New Pool Name.** Enter a unique name for the new pool that you wish to create.*
2. Allocate all available disk space by leaving the **Auto Configuration** and **Maximize Size** box checked within the **Pool Mapping Preference** section.
3. Click on **Create Pool.**

- To manually allocate Disk Space to the new Pool select **Manual Configuration** within the **Pool Mapping Preference** section and assign the desired size (gigabytes) by using the slider.

*Please note that disk space must be available to create a New Pool. If one pool is using all available disk space (default setting) you must resize the pool prior to creating a New Pool. Please see the "Resize Pool" section and follow the instructions.

Creating a Mirrored Pool*

Often referred to as RAID 1, a Mirrored Pool allows you to create multiple copies of data. Each drive within a Mirrored Pool contains the exact same information and is updated each time the primary disk or "Base" is saved. To create a Mirrored Pool follow the steps below.

1. Within the **Disk Management** menu, select **Create New Pool**
2. **New Pool Name.** Enter a unique name for the new pool that you wish to create.
3. Select the **Mirroring** check box.
   - If you wish to have the DiskGO determine which device is the base and which is the Mirror, check the **Auto Configuration** box within **Pool Mapping preferences** and move on to Step 4. The auto configuration will automatically designate the drive with the least amount of available space as the Base and the drive with the greater amount of space as the Mirror. If you wish to manually select which drive is the Base and which is the Mirror select **Manual Configuration** within the **Pool Mapping Preferences** section and move on to Step 5. .
4. To set the size of the Mirror to the size of the Base select **Maximize Size.** To manually specify the amount of space uncheck **Maximize Size,** select the desired capacity (gigabytes) and click on **Create Pool.**
5. Assign the appropriate disks to be used as the Base and Mirror within **Disk Assignment.** Within **Space Allocation** enter the desired size (gigabytes) of the base using the slider. Click on **Create Pool.**

*An external hard drive must be connected to the DiskGO via USB in order to utilize a Mirrored Pool. The attached drive must also be greater than or equal to the size of the pool you wish to Mirror.

Creating Striped Pool*

Often referred to as RAID 0, the primary purpose is to increase performance. It is important to realize that Striping does not create multiple copies of the Data like a Mirror and therefore does not protect against data loss if a drive were to fail.

1. Within the **Disk Management** menu, select **Create New Pool**
2. **New Pool Name.** Enter a unique name for the new pool that you wish to create.
3. Select the **Striping** check box.
4. Select the # of external disks to be included in the Striped pool within the **Number of Stripes** section.
   - If you wish to have the DiskGO configure the pools automatically check the **Auto Configuration** box within **Pool Mapping preferences** and move on to Step 5. If you wish to manually configure the drives select **Manual Configuration** within the **Pool Mapping Preferences** section and move on to Step 6.
5. To utilize all available disk space select **Maximize Size**. If you wish to allocate space manually uncheck **Maximize Size** and enter the desired amount of space per Stripe (gigabytes) within the **Space Allocation** section. Click on **Create Pool.**
6. To manually configure the drives assign the appropriate drive number within **Drive Assignment** (Stripe 0, Stripe 1 and Stripe 3). Enter the desired amount of space per Stripe (gigabytes) within the **Space Allocation** section. Click on **Create Pool.**

*An external hard drive or drives must be connected to the DiskGO via USB in order to utilize a Striped Pool.

Encrypting the Pool

Encrypting pools provides security for all data stored within that specific pool. Encrypted pools must be mounted (see "Remounting an Encrypted Pool") each time the DiskGO is rebooted, powered off, restored, or removed from the network. The following steps should be used to encrypt a pool:

1. Within the **Disk Management** menu, select **Create New Pool**
2. **New Pool Name.** Enter a unique name for the new pool that you wish to create.
3. Select the **Encrypt Pool** check box.
4. Enter a unique password within **Encryption Password.** Note that only alphanumeric characters may be used. The password also should be at least 8 characters long.
5. Re-enter the password within the **Confirm Password** field**.**
6. Allocate all available disk space by leaving the **Auto Configuration** and **Maximize Size** box checked within the **Pool Mapping Preference** section. Click **Create Pool.** Or to manually allocate Disk Space to the new Pool select **Manual Configuration** within the **Pool Mapping Preference** section and assign the desired size (gigabytes) by using the slider. Click **Create Pool.**

Changing the Encryption Password

1. Select **Basic** from the **Disk Management** menu.
2. Within **Disk Pool Mapping** select **Change Encryption**
3. Select the pool you wish to change from the **Encrypted Pool Name** list.
4. Select **Enable Pool Encryption** from **Encrypt Pool**
5. Enter the new password within the **New Password** and **Confirm Password** fields. Note that only alphanumeric characters may be used. The password also should be at least 8 characters long. Select **Change Encryption**

Disabling Pool Encryption

1. Select **Basic** from the **Disk Management** menu.
2. Within **Disk Pool Mapping** select **Change Encryption**
3. Select the pool you wish to change from the **Encrypted Pool Name** list.
4. Select **Enable Pool Encryption** from **Encrypt Pool**
5. Leave both **New Password** and **Confirm Password** blank. Select **Change Encryption.**

Remounting Encrypted Shares

Encrypted pools must be mounted each time the DiskGO 3.5” Network Hard Drive is rebooted, powered off, restored, or removed from the network. Follow the steps below to remount an encrypted pool.

1. Select **Basic** from the **Disk Management** menu.
2. Click on the **Enter Encryption Password** button from the **Disk Pool Mappings** section for each encrypted drive you want to mount.
3. Enter the passwords for each pool within **Encrypted Pool Names** and select **Mount Pools.**

RESIZING POOL*

1. Open the **Resize Disk Pool** page from the **Disk Management** menu.
2. Click the name of the disk pool that you wish to change in the **Pool Name** list.
3. In the **Space Allocation** boxes, type the amount of allocation space (gigabytes), or use the slider to specify the allocation space for each pool.
4. Click **Resize Pool**.

*Pools cannot be reduced in capacity to a size less than the space consumed by the shares within the pool.

ADD MIRRORS

If additional disks are available, you can add mirrors to existing pools. Also, you can convert a JBOD (just a bunch of disks) pool to the mirror pool. To add mirrors/spares, follow the steps below.

1. Open the **Add Mirrors** page from the **Disk Management** menu
2. Select the pool you wish to mirror from the **Pool Name** field
3. Select the mirror device from the **Mirroring** field

4. Select the number of mirrors from the **Number of Additional Mirrors** field. **Note**: the number of mirrors must be equal to the number of additional physical disks connected to the DiskGO drive.
5. Within **Disk Assignment** select the appropriate checkbox for the drive where the mirror will be stored. Select **Add Mirrors.**

REMOVE MIRRORS

On the Remove Mirrors/Spares page, you can remove mirrors/spares from existing pools. If one of the disks of a mirrored pool has failed, you must use this page to remove the mirror from the pool.

1. Open the **Remove Mirrors** page from the **Disk Management** menu
2. Select the pool you wish to change from the **Pool Name** field
3. Select the mirror device from the **Available Mirrors** list and select **Remove Mirrors.**

POWER MANAGEMENT

On the Disk Power Management page, you can modify the spin down times of the available disks when they are idle. The times specified can be given in 5-second intervals up to a maximum of 5 hours 30 minutes.

NETWORKING

LAN

The default IP addressing for the DiskGO 3.5" Network Hard Drive is as a DHCP client. Most networks and gateways use DHCP protocols to assign IP address to connected devices. The DHCP client setting will allow the network to automatically assign an IP address to the DiskGO. If you wish to change this setting to **DHCP Server** or **Static IP** follow the steps below.

DHCP Server

This setting will change the DiskGO from a client accepting an IP address from the network to a providing IP addresses to other devices (computers, servers, printers, etc.) connected to the Network. By changing this setting it may make it necessary to change some network and other DHCP settings manually. To change the DiskGO to a DHCP Server follow the steps below.

1. Select **LAN** from the **Networking** menu
2. Select **DHCP Server** from the **LAN Protocol** dropdown list.
3. Within **LAN IP Address** enter a static IP address for the DiskGO. Make certain that the IP address selected is on the same LAN segment as the computer running Administrator.
4. Set the IP address as necessary to function on your network:
   - LAN Domain Name
   - LAN DNS Servers (preferred and 2 alternates)
   - LAN WINS Servers (preferred and 2 alternates)
5. Click **Apply** and **Continue**

Static IP

Static IP allows you to assign a fixed IP address to the DiskGO. Be advised that all other devices connected to the network must also be configured with a Static IP address in order to connect to the DiskGO. The following steps need to be followed to set the DiskGO to Static.

1. Select **LAN** from the **Networking** menu
2. Select **STATIC** from the **LAN Protocol** dropdown list.
3. **Disable** the **LAN IP** from the **Autoconfiguration** list
4. Set the IP address as necessary to function on your network:
   - LAN IP Address
   - LAN Subnet Mask
   - LAN Default Gateway
   - LAN Domain Name
   - LAN DNS Servers (preferred and 2 alternates)
   - LAN WINS Servers (preferred and 2 alternates)
5. Click **Apply** and **Continue**

PRINTERS

On the Printers page, you can select a printer pool to install printer services, and to view information about the printers that are connected to the DiskGO. You can assign a name for the printer or allow the printer installer to assign the name based on the printer model. Please note when printer services are being configured, the DiskGO is briefly unavailable to client users. Therefore, configuring printer services is recommended as part of a planned update. Also each computer that will be accessing the printer via the DiskGO 3.5" Network Hard Drive must have the printer driver installed (see "Adding Printers in Windows").

Setting the DiskGO as a Print Server

1. Open the **Printers** page from the **Printers** menu.
2. In the **Printer Pool Name** list, click the name of the pool in which to install printer services.
3. Connect a USB printer to the USB port on the DiskGO and confirm that the printer is turned on.

4. In the **Connected Printers** list, select the name of the connected printer and click **Apply.**

Adding the Printer in Windows

1. Open Windows Explorer and browse to the DiskGO folder.
2. Double-click **Printer and Faxes**.
3. Right-click the name of the printer you want to add, and then click **Connect**.
4. Click **OK** on the message "**The server for the printer does not have the correct printer driver installed. If you want to search for the proper driver, click OK."**
5. Follow the instructions provided by the **Add Printer Wizard**.

6. Repeat this procedure on each additional client computer.

Printer Troubleshooting

The printer driver was successfully installed but I can’t print to the printer.

Recommended action

1. On your Windows client computer, open **Printers and Faxes** in **Control Panel**.
2. Right-click the name of the printer icon, and then click **Properties.**
3. Click the **Advanced** tab, and then click **Print Processor**.
4. Change the print processor to **WINPRINT** if it is not already set to it.